DIGITAL TRUST AND REPUTATION: APPLICATIONS AND SECURITY ISSUES

BY

YUHONG LIU

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN DEPARTMENT OF ELECTRICAL, COMPUTER AND BIOMEDICAL ENGINEERING

UNIVERSITY OF RHODE ISLAND

2012

Library Rights Statement

In presenting this dissertation in partial fulfillment of the requirements for an advanced degree at the University of Rhode Island, I agree that the Library shall make it freely available for inspection. I further agree that permission for copying, as provided for by the Copyright Law of the United States (Title 17, U.S. Code), of the dissertation for scholarly purposes may be granted by the Librarian. It is understood that any copying or publication of this dissertation for financial gains shall not be allowed without my written permission.

I hereby grant permission to the University of Rhode Island Library to use my dissertation for scholarly purposes.

_____

Signature

_____

Date

DOCTOR OF PHILOSOPHY DISSERTATION

OF

YUHONG LIU

APPROVED:

Dissertation Committee:

Major Professor _____

_____

_____

_____

DEAN OF THE GRADUATE SCHOOL

UNIVERSITY OF RHODE ISLAND

2012

ABSTRACT

Digital Trust borrows the trust concept in sociology to indicate that, in distributed computing and communication systems, one party evaluates whether other parties are trusted to perform a certain action or have a certain property. When the digital trust value is published to an entire network or to general users, it is called digital reputation. This dissertation investigates the security issues in digital trust and reputation systems in the context of online social networks and explores a new application of digital trust in biomedical sensor systems. Specifically, the study consists of three parts:

Anomaly detection in feedback-based reputation systems through temporal and correlation analysis

As more people use the Internet for entertainment, building personal relationships, and conducting businesses, how to evaluate strangers' quality or trustworthiness in online systems becomes an important issue. Online reputation systems, also referred to as online rating systems, allow users to post their ratings/reviews on items in the system, aggregate these ratings/reviews, and assign each item with a reputation score that indicates its quality. The items that receive user ratings can be *products* (e.g. in the Amazon product rating system), *services* (e.g. hotel ratings in various travel sites), *users* (e.g. sellers and buyers at eBay), and *digital content* (e.g. video clips at YouTube). Online reputation systems can help people evaluate the quality of online items before transactions, and hence greatly reduce the risks of online interactions.

Due to the high influence of online reputation systems, attacks that attempt to mislead users' online decisions through dishonest ratings/reviews are gaining popularity. Sellers at the online marketplace boost their reputation by trading with collaborators. Firms post biased ratings and reviews to praise their own products

or "bad-mouth" the products of their competitors. Scammers are making profits by writing sophisticated programs to automatically insert feedbacks. Attacks against reputation systems can overly inflate or deflate item reputation scores, crash users' confidence in online reputation systems, eventually undermine reputation-centric online businesses and lead to economic loss.

In this part, we propose TAUCA, short for joint Temporal And User Correlation Analysis. It identifies malicious users and recovers reputation scores from a novel angle: combination of temporal analysis and user correlation analysis. Benefiting from the rich information in the time-domain, TAUCA identifies the products under attack, the time when attacks occur, and malicious users who insert dishonest ratings. TAUCA and two other representative schemes are tested against real user attack data collected through a cyber competition. TAUCA demonstrates significant advantages. It largely improves the detection rate and reduces the false alarm rate in the detection of malicious users. It also effectively reduces bias in the recovered reputation scores.

Defending multiple-user-multiple-target attacks in online reputation systems

Driven by the huge profits of online markets, reputation manipulations have evolved rapidly. Nowadays, some powerful attacks are conducted by companies that make profit through manipulating the reputations of online items for their customers. We define this type of attacks as multiple-user-multiple-target attacks. Compared to the single-target attacks addressed in the previous part, the multiple-target attack usually has larger attack power while it is relatively new to the research community. Very limited work has been done to address it. To address these attacks, we propose a defense scheme that (1) sets up heterogeneous thresholds for detecting multiple suspicious items and (2) identifies target items based

on correlation analysis among suspicious items. The proposed scheme and two other comparison schemes are evaluated by a combination of real user data and simulation data. The proposed scheme demonstrates significant advantages in detecting malicious users, recovering reputation scores of target items, and reducing interference to normal items.

Note that the concept of "correlation" in this thesis is not as same as the strict definition of correlation in statistics. Given two users, we consider these two users' rating behaviors as two random variables, compute the Euclidean distance between these two random variables and take its inverse as the correlation value between these two given users. Furthermore, the item correlation is calculated by combining user correlation values among users who rate these two items. The concepts of user correlation and item correlation in this thesis are actually introduced to measure the similarity among users and among items.

Trust sensor interface for improving reliability of EMG-based user intent recognition

In the above two parts, we studied how to build up secure and reliable digital trust and reputation systems. The next question is that: can we apply this secure and reliable trust and reputation systems in other fields, such as biomedical sensor systems? In such systems, signals obtained from sensors are the basis for monitoring patients' status and making medical decisions. Therefore, ensuring the reliability of sensors is critically important. The digital trust mechanism which dynamically evaluates the reliability of a given object inherently fits in this field. Specifically, we apply the digital trust approach on a neural-machine interface for artificial legs.

To achieve natural and smooth control of prostheses, Electromyographic (EMG) signals have been investigated for decoding user intent. However, EMG

signals can be easily contaminated by diverse disturbances, leading to errors in user intent recognition and threatening the safety of prostheses users. To address this problem, we propose a trust sensor interface (TSI) that contains 2 modules: (1) abnormality detector that detects diverse disturbances with high accuracy and low latency and (2) trust evaluation that dynamically evaluates the reliability of EMG sensors. Based on the output of the TSI, the user intention recognition (UIR) algorithm is able to dynamically adjust their operations or decisions. Our experiments on five able-bodied subjects and two amputee subjects have demonstrated that the proposed TSI can effectively detect two types of disturbances, motion artifacts and baseline shifts, and improve the reliability of the UIR.